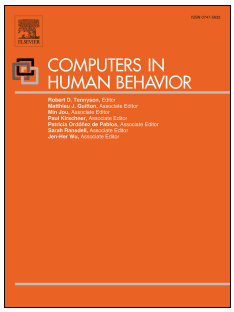
Journal Pre-proof



Employees' behavioural intention to smartphone security: A gender-based, cross-national study

Nisreen Ameen, Ali Tarhini, Mahmood Hussain Shah, Nnamdi Madichie

PII: S0747-5632(19)30396-6

DOI: https://doi.org/10.1016/j.chb.2019.106184

Reference: CHB 106184

To appear in: *Computers in Human Behavior*

Received Date: 16 May 2019

Revised Date: 26 October 2019

Accepted Date: 29 October 2019

Please cite this article as: Ameen N., Tarhini A., Hussain Shah M. & Madichie N., Employees' behavioural intention to smartphone security: A gender-based, cross-national study, *Computers in Human Behavior* (2019), doi: https://doi.org/10.1016/j.chb.2019.106184.

This is a PDF file of an article that has undergone enhancements after acceptance, such as the addition of a cover page and metadata, and formatting for readability, but it is not yet the definitive version of record. This version will undergo additional copyediting, typesetting and review before it is published in its final form, but we are providing this version to give early visibility of the article. Please note that, during the production process, errors may be discovered which could affect the content, and all legal disclaimers that apply to the journal pertain.

© 2019 Published by Elsevier Ltd.

Journal Pre-proof

Title: Employees' behavioural intention to smartphone security: A gender-based, cross-national study

Paper type: Full length article

Author names and affiliations

Author 1 Name: Nisreen Ameen
Department: School of Management
University/Institution: Royal Holloway, University of London
Town/City: London
Country: United Kingdom

Author 2 Name: Ali Tarhini
Department: Department of Information Systems
University/Institution: Sultan Qaboos University
Town/City: Muscat
Country: Oman

Author 3 Name: Mahmood Hussain Shah
Department: School of Strategy and Leadership
University/Institution: Coventry University
Town/City: Coventry
Country: United Kingdom

Author 4 Name: Nnamdi Madichie
Department: School of Business, Law and Social Sciences,
Dundee Business School
University/Institution: Abertay University
Country: United Kingdom

Corresponding author
Dr. Nisreen Ameen

Corresponding author's email
nisreen.ameen@rhul.ac.uk

Corresponding author's mobile number
(0044) 07455005059

Corresponding author's address:

Journal Pre-proof

Journal Pre-proof

Royal Holloway, University of London

School of Management

Egham

TW20 0EX

Declaration of Interest: none

We wish to confirm that there are no known conflicts of interest associated with this publication and there has been no significant financial support for this work that could have influenced its outcome.

Journal Pre-proof

Journal Pre-proof

Employees' behavioural intention to smartphone security: A gender-based, cross-national study

Abstract

Despite the benefits of bring your own device (BYOD) programmes, they are considered one of the top security risks companies are facing. Furthermore, there is a gap in the literature in understanding gender differences in employees' smartphone security behavioural intention. This research analyses gender differences in smartphone security behavioural intention among employees in the United Arab Emirates (UAE) and the United States (US). The research develops a new model, the behavioural model of cybersecurity (BMS), based on a combination of the protection motivation theory (PMT), the general deterrence theory (GDT) and Hofstede's cultural dimensions. A questionnaire was distributed to employees in both countries. A total of 1156 usable responses were analysed using partial least squares-structural equation modelling. The findings show that gender differences exist, but neither male nor female employees in either country are aware of the risks associated with their use of smartphones, despite their awareness of the existence of their company's BYOD security policies. The research provides theoretical and practical contributions by developing a new model combining the PMT, GDT and Hofstede's cultural dimensions and suggests gender differences in employees' smartphone security behavioural intention in a cross-national context. It has several practical implications for practitioners and policymakers.

Keywords: BYOD security; PMT; GDT; smartphone security; employees' BYOD security intention; Hofstede's cultural dimensions

1. Introduction

The use of mobile phones, smartphones, laptops and tablets by employees for work purposes is often referred to as bring your own device (BYOD). Previous studies showed that one of the major issues associated with the use of BYOD is managers' inability to ensure that companies' data is kept secure as these devices are used both for personal and professional/work purposes combined (Baillette, Barlette, & Leclercq-Vandelannoitte, 2018; Bautista, Rosenthal, Lin, & Theng, 2018; Brown & Palvia, 2015). This makes controlling how employees use these devices a challenge for companies (Baillette et al., 2018; Bautista et al., 2018). The BYOD security market is expected to grow to approximately US$69 billion by 2023, at 37% of the compound annual growth rate between 2018 and 2023 (Heraldkeeper, 2019). Hence, there is a growing business concern about the threats posed by these devices. Businesses that have staff using BYOD are 49% more likely than average to experience security breaches (Vaidya, 2018).

The smartphone is the most widely used device in the world. The opportunities associated with the use of smartphones are endless. The smartphone is a platform for many different types of mobile applications that can be used for different purposes (Ameen & Willis, 2018a). The features of the smartphone along with the different mobile applications that can be accessed through it provide new opportunities for businesses as employees use these applications in a variety of ways (Pitichat, 2013). The use of smartphones offers benefits to both organisations and employees. The benefits of allowing employees to use their personal smartphones for work purposes are valued by businesses (Hamblen, 2015). Smartphones allow companies to reach their employees faster, reduce cost, manage the business more effectively with the use of different mobile applications and mobile dashboards, and experience a more effective and faster knowledge sharing (Baillette et al., 2018; Maitlo, Ameen, Peikari, & Shah, 2019; Pitichat, 2013). From the employees' perspective, the use of

Journal Pre-proof

smartphones helps to improves communication between employees, provide autonomy, improve relationships and increase the level of flexibility and reach (Pitichat, 2013). Companies that favour BYOD and have a BYOD security policy in place make an annual saving of US$350 per year per employee (Bullock, 2019). In addition, the use of BYOD for work purposes saves employees 58 minutes per day and increases productivity by 34% (Bullock, 2019).

The lack of employees' security awareness when using BYOD for work purposes remains a major challenge for companies (Doargajudhur & Dell, 2019; Timms, 2017). This is especially the case in the context of employees' use of smartphones as these devices can be used mainly for personal but also for work purposes (Baillette et al., 2018; Bautista et al., 2018; Köffer, Ortbach, & Niehaves, 2014). This makes it difficult for companies to control how and where their data is being accessed. Although some companies initiate BYOD policies, these policies are generic and do not account for the different types of devices, operating systems and mobile applications that employees use in a workplace (Gregory, 2018). The diverse types of mobile devices and operating systems that employees usually use create a major challenge for organisations (Gregory, 2018). The use of smartphones can present various risks to organisations, for example, malware, data leakage, theft or loss of mobile devices, network connectivity of the device (such as Wi-Fi and Bluetooth) and the use of different web-based and mobile applications as mobile device users usually download applications which are of interest to them onto their mobile devices (Weber & Rudman, 2018).

Employees' information security compliance behaviour includes complying with information security policies, promoting security assurance behaviour and helping to prevent unacceptable information behaviour among employees within an organisation (Guo, 2013; Humaidi & Balakrishnan, 2015). Previous research studied employees' security behaviour when using BYOD at work (e.g. Al Askar & Shen, 2016; Arpaci, 2019; Baillette et al., 2018; Bulgurcu, Cavusoglu, & Benbasat, 2010; de las Cuevas et al., 2015; Disterer & Kleiner, 2013; Hovav & Putri, 2016; Kerr, Talaei-Khoei, & Ghapanchi, 2018; Martens, De Wolf, & De Marez, 2019; Musarurwa, Flowerday, & Cilliers, 2017; Dang-Pham & Pittayachawan, 2015; Romer, 2014; Zahadat, Blessner, Ubene, Agim, & Umo-Odiong, 2015). However, there is a gap in the existing literature in terms of research accounting for gender differences in BYOD security behavioural intention in the workforce.

Previous research highlighted significant differences between men and women in terms of the adoption of, use and interaction with different technologies including smartphones (Ameen, Willis, & Shah, 2018; Ameen & Willis, 2018b; Bhandari, 2019; Lin, Featherman, Brooks, & Hajli, 2018; Tarhini, Elyas, Akour, & Al-Salti, 2016). Hence, it is important to study the differences between male and female employees in terms of their security behavioural intention when using smartphones for work purposes. The role of women is changing in both developed and developing countries (Madichie & Gallant, 2012). Women form almost half of the workforce in many countries in the world (Fetterolf, 2018). The discussion of women in the workforce has been undertaken in terms of their contribution to the workforce in Middle Eastern contexts (Fetterolf, 2018; Madichie & Gallant, 2012). In addition, there is a lack of research that identifies gender differences in employee's smartphone security behavioural intention in a cross-national/cultural context to reveal the similarities and differences in their behavioural intention. This is important due to the dramatic increase in the number of global companies employing teams from different parts of the world (PWC, 2017), especially in the US, China, and more recently the United Arab Emirates (UAE) (Gulf News, 2015; PWC, 2017). Hence, it is vital for these companies to build a good understanding of their

Journal Pre-proof

employees' smartphone security behavioural intention and any gender differences involved to develop more effective policies.

The main aim of this study is to analyse gender differences in terms of the factors that can affect employees' smartphone security behavioural intention when using smartphones for work-related activities in a cross-national/cultural context, namely, in the US and UAE. This research contributes to the existing literature in many ways. First, this is the first research to study gender differences in terms of employees' security behavioural intention when using smartphones for work-related activities. Second, the research investigates gender differences in terms of employees' smartphone security behavioural intention in a cross-national context, taking examples from the US and UAE. Third, the research contributes to the existing literature by proposing the behavioural model of cybersecurity (BMS), which combines the protection motivation theory (PMT) (Maddux & Rogers, 1983; Rogers, 1975; Rogers, 1983),the general deterrence theory (GDT) (Beccaria, 1963), and Hofstede's cultural dimensions (Hofstede, 1980) to reveal how male and female employees' espoused national cultural values affect their smartphone security behavioural intention. In addition to the theoretical contributions, this research has practical implications for global companies operating in many countries to understand gender differences in smartphone security behaviour among their employees and develop more effective policies that account for employees' views.

Following this opening section, the next section provides the literature review including a background on the use of BYOD and organisational cybersecurity policies in the two countries and a review of recent studies that focused on employees' BYOD security behaviour. Then, the theoretical model and proposed hypotheses are presented. This is followed by the methodology, data analysis and results. Then, the discussion and the theoretical and practical contributions of the research are provided. Finally, the conclusion, limitations and areas for future research are presented.

2. Literature review

2.1 BYOD security in the US and UAE

The US government has described cybersecurity as "one of the most serious economic and national security challenges we face as a nation." (Kaplan, Sharma, & Weinberg, 2011). Out of 70 million devices lost every year, only 7% were recovered, while 76% of US companies do not encrypt mobile devices (Lord, 2017). In the US, 90% of employees use their smartphones for work, 40% of large data breaches were caused by a loss of a device and 60% of companies do not remove business data from their ex-employees' devices (Lord, 2017). Nearly half of businesses in the US have no formal BYOD policy for their employees to follow (Hamblen, 2015). The US female labour participation rate is more than half (United States Department of Labor, 2019). Hence, female employees form an important segment of the US workforce.

Despite the UAE being reportedly a digital business hub, the need for firms to address BYOD security issues caused by their employees' behaviour has been highlighted as a major issue (Buller, 2018). Nearly 83% of employees in the UAE have already harnessed remote working in some form (Trade Arabia, 2016). In addition, 44% of IT decision makers cited security of mobile devices as the top reason for not promoting mobile work further (Trade Arabia, 2016). The number of female employees in the UAE has been accelerating rapidly in both public and private sectors (Badam, 2018). Of female Emiratis, 13.3% occupy senior positions (Dubai Government Centre, 2019). Table 1 provides a comparison between the US and UAE in smartphone use and female labour participation rate.

Journal Pre-proof

Table 1. Comparison between US and UAE in BYOD use and women participation rate

Criteria	US	UAE
Share of businesses where BYOD occurs	87%	45%
Female labour force participation rate	56%	29%
Smartphone adoption rate	77%	83%
Ranking of commitment to cybersecurity	2nd	47th

Sources: GSMA, 2017; Lazar, 2018; Pewinternet, 2018; Trade Arabia, 2016; World Bank, 2018

In addition to the reported differences between the two countries in terms of female labour participation rate (Madichie & Gallant, 2012), smartphone adoption rate and their ranking of commitment to cybersecurity, these countries score differently in terms of culture. Table 2 provides a comparison between the two countries with reference to Hofstede's cultural dimensions: power distance, uncertainty avoidance, masculinity vs femininity and individualism vs collectivism (Hofstede, 2019).

Table 2. Comparison between US and UAE in cultural characteristics

Dimension	US	UAE
Power distance	90	40
Uncertainty avoidance	80	46
Masculinity vs femininity	50	62
Individualism vs collectivism	25	91

Source: Hofstede, 2019

There are many reasons for selecting these two countries. First, female employees play an important role in the workforce in these two countries. Over half of the total number of employees in the US (56%) are female and 29% of employees in the UAE are female (World Bank, 2018), with a good potential to increase rapidly in the UAE in the next few years (Haine, 2017). Second, these two countries represent a good hub for global business and global companies to operate (Gulf News, 2015; PWC, 2017). Third, these countries are different in terms of their cultural characteristics and how women work, and business ethics. Fourth, they rank differently in terms of commitment to cyber security as the US is ranked 2nd and UAE is ranked 47th (International Telecommunication Union, 2017). Fifth, they score differently in each of the four main Hofstede cultural dimensions (Table 2). Therefore, comparing gender differences in smartphone security behaviour in these two countries may reveal interesting and useful findings.

2.2 Gender and BYOD employee security behaviour research

The role of gender differences in cybersecurity research is not clearly defined. Previous studies showed that there is a gap in existing literature in terms of the differences between men and women in deterrence (Carmichael, 2004; Chen, Wu, Chen, & Teng, 2018). The need for further research investigating gender differences between employees' information systems security behavioural intention has been identified in previous studies (Chen et al., 2018; Gratian, Bandi, Cukier, Dykstra, & Ginther, 2018; Hadlington, 2018). Previous studies investigated gender differences in employees' cybersecurity behaviour (e.g. Akman & Mishra, 2010; Ifinedo, 2014; Ifinedo, 2016; Foth, 2016; Anwar et al., 2017; McCormac et al., 2017; Mamonov & Benbunan-Fich, 2018; Hadlington, 2018; Gratian et al., 2018; Chen et al., 2018). Nevertheless, despite the literature being rich in studies investigating employees' information security behaviour, there is a gap in the literature in three areas. First, there is an

Journal Pre-proof

absence of focus on female employees' perceptions on BYOD and more specifically, smartphone security behaviour. Second, there is a gap in the existing research in terms of focusing on the differences between male and female employees in a cross-national context, comparing countries which score differently in terms of the cybersecurity index to understand the differences and similarities between them. Third, there is a lack of studies that test gender differences in terms of how male and female employees' espoused national cultural values affect their BYOD (smartphone) security behavioural intention. This research aims to address these gaps in the literature.

3. Conceptual model

The literature is rich with models used in the area of cybersecurity (van Bavel, Rodríguez-Priego, Vila, & Briggs, 2019). One of the most cited theories in this area is PMT, which seeks to clarify the cognitive processes which mediate behaviour in the face of a threat (Rogers, 1975, 1983; van Bavel et al., 2019). The theory focuses on two appraisal processes. First, it focused on the threat itself. Second, it focuses on companies' ability to act against that threat (threat appraisal and coping appraisal, respectively). The theory illustrates that humans are more motivated to be protective when they are aware of the existence of the threat, the level of the threat and the consequences (Chen et al., 2018). The theory integrates five main factors: perceived risk vulnerability, severity of the adverse consequences, perceived response efficacy, perceived self-efficacy and response cost. It has been applied in different areas of cybersecurity including protective behaviour from viruses (Lee, LaRose, & Rifon, 2008), home computer users protecting their computers (Anderson & Agarwal, 2010), response to fear appeal by employers' security behaviour (Johnston & Warkentin, 2010) and intentions towards taking security measures against malware, scams and cybercrime (Martens et al., 2019). Recent studies adopted the PMT in the context of BYOD security behaviour (e.g. Putri & Hovav, 2014; Tu, Adkins & Zhao, 2018; Al Askar & Shen, 2016; Hovav & Putri, 2016; Han, 2017; Dang-Pham & Pittayachawan, 2015; Crossler & Bélanger, 2017; Blythe and Coventry, 2018). The analysis of these studies shows that there is a gap in research in terms of understanding gender differences in employees' smartphone security behaviour in a cross-national context and in accounting for the role of culture.

Similar to PMT, the GDT has been used as a theoretical foundation in information security research and it is rooted to fear appeal (Chen et al., 2018). The theory suggests that when a fear appeal in the form of policy is presented to individuals, they will evaluate the advantages and risks of violating the rules outlined in the fear appeal (Chen et al., 2018; Jacobs, 2010). The theory focuses on two main aspects of sanctions including the severity of sanctions and the certainty of sanctions (Merhi & Ahluwalia, 2019). It focuses on punishment severity and its effects on individuals' security behaviour by creating fear through focusing on punishment severity and certainty (Merhi & Ahluwalia, 2019). The theory illustrates that punishments are more effective than norms in terms of information security behaviour.

Previous research combined PMT and GDT to investigate issues in cybersecurity (e.g. Herath & Rao, 2009a; Siponen, Pahnila, & Mahmood, 2006). However, the GDT has not been applied in the context of investigating gender differences in employees' BYOD (smartphone) security behaviour. The integration of both theories is justified as it provides a more informative view of appraisal and fear combined. In addition, culture can play an important role in individuals' behaviour in both organisational and voluntary settings.

Journal Pre-proof

Culture has been defined as "The collective programming of the mind that distinguishes the members of one group or category of people from others" (Hofstede, 2019). Despite previous research studying the effects of organisational culture on cybersecurity behaviour (e.g. Connolly, Lang, Gathegi, & Tygar, 2017; Greene & D'Arcy, 2010; Übelacker, 2013), there is a gap in the literature in terms of investigating how male and female employees' espoused national cultural values can affect their BYOD (smartphone) security behavioural intention. Reportedly, Hofstede's cultural dimensions have been investigated in the existing literature focusing on the effect of culture on cybersecurity behaviour (Björck & Jiang, 2006; Onumo, Cullen, & Ullah-Awan, 2017).

National culture is a macro-level phenomenon. However, employees' smartphone security behaviour is an individual-level phenomenon, which may not be determined by national and organisational culture. Individual behaviour cannot be measured or predicted using a national measurement score, as there are no means to generalise cultural characteristics of individuals within the same country (Hoehle, Zhang, & Venkatesh, 2015; Srite & Karahanna, 2006). There is a lack of research on the effects of employees' espoused national cultural values as represented by Hofstede's cultural dimensions. Furthermore, versions of Hofstede's instrument at the individual level should be used with research models at the individual level (McCoy, Everard, & Jones, 2005). This approach has been used in studies on culture and technology adoption among individuals (Srite & Karahanna, 2006; Tarhini, Hone & Liu, 2015). Hence, this study focuses on employees' espoused national cultural values (i.e. espoused national cultural values at the individual level) to provide a more informative view of their BYOD (smartphone) security behavioural intention. Individuals with different espoused national cultural values are likely to perceive BYOD security behaviour in different ways. Table 3 provides the key definitions of each of these dimensions.

Table 3. Key definitions of Hofstede's cultural dimensions

Dimension	Definition
Uncertainty avoidance	The extent to which the members of a culture feel threatened by ambiguous or unknown situations and have created beliefs and institutions that try to avoid these.
Power distance	The extent to which the less powerful members of institutions and organisations within a country expect and accept that power is distributed unequally.
Individualism vs collectivism	The degree of interdependence a society maintains among members of a culture.
Masculinity vs femininity	What motivates people, wanting to be the best (Masculine) or liking what you do (feminine).

Source: Hofstede, 2019

In order to achieve our aim of analysing gender differences in employees' intention towards BYOD (smartphone) security behaviour, we propose a new model, the BMS, which combines the PMT, GDT and Hofstede's cultural factors. Combining these theories with cultural dimensions provides a better understanding of gender differences in employees' BYOD (smartphone) security behavioural intention.

4. Hypothesis development

The following subsections provide the hypotheses developed in this study. The research model of this study is depicted in Figure 1.

Journal Pre-proof

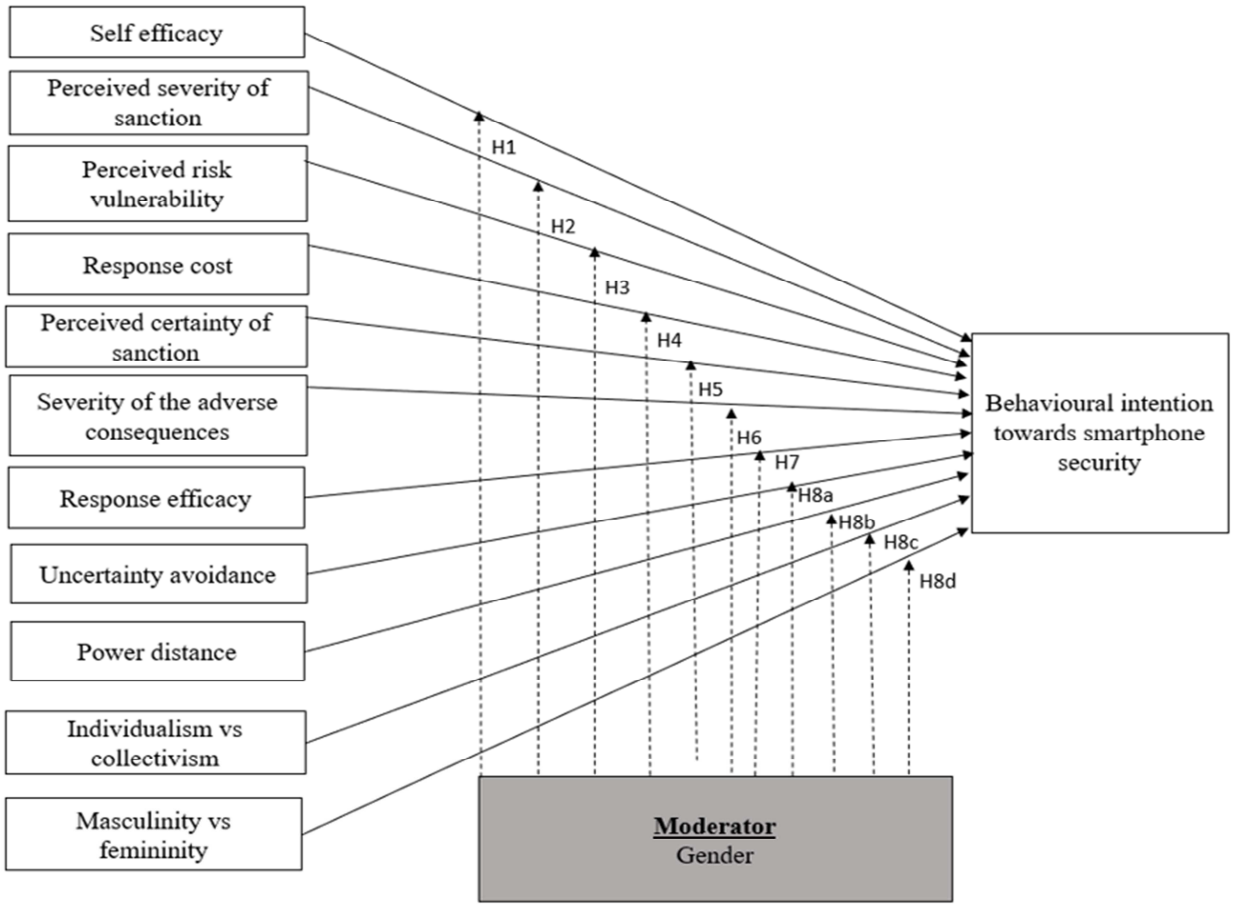


Figure 1. Proposed research model

4.1 Self-efficacy

Self-efficacy is one of the key aspects of human activity, including interaction with technology and security (Latikka, Turja, & Oksanen, 2019). Previous studies showed that males are generally more confident with the use of technology than females (He & Freeman, 2010). Women are socialised in such a way that they do not have access to the information necessary to develop the self-efficacy beliefs (Zeldin, Britner, & Pajares, 2008). This is possibly due to the higher frequency of interaction that men have with technology (King, Bond, & Blandford, 2002), including smartphones, which makes them more aware of the issues around the use of that technology. Individuals may have serious doubts about whether they can perform a task if they are not sufficiently exposed to technology, which may prevent them from completing the task (He, Chen, & Kitkuakul, 2018). Previous studies revealed that being exposed to technology and sharing knowledge about it helps to increase individuals' self-efficacy in using it (He et al., 2018). Because men are more likely to have this exposure, they have higher self-efficacy with regard to using technology than women do (Koch, Muller, & Sieverding, 2008; Ong & Lai, 2006; Wong, Teo, & Russo, 2012). Therefore, due to the psychological effects of this belief on their behaviour, male employees' belief in their ability to keep their smartphones secure can be a predictor of their behavioural intention towards smartphone security. A higher level of self-efficacy increases employees' behavioural intention to ensure the security of their smartphones. Hence, we propose the following hypothesis:

Journal Pre-proof

H1. Self-efficacy has a more significant effect on behavioural intention towards smartphone security behaviour among male employees than female employees.

4.2 Perceived severity of sanction

Previous studies show that perceived severity of sanction has a negative effect on information systems misuse intention (Cheng, Li, Li, Holm, & Jai, 2013; D'Arcy, Hovav, & Galletta, 2009; Willison, Warkentin, & Johnston, 2018). The higher employees perceive the severity of sanction, the less likely they will violate information security policies (Alshare, Lane, & Lane, 2018). The first possible punishment that can increase employees' intention towards information systems security is managerial sanctions, followed by legal sanctions (Kobayashi & Grasmick, 2002). Previous studies on gender differences in criminology showed that females are more afraid of punishment than males (Hale, 1996; Callanan & Teasdale, 2009). Hence, we propose the following hypothesis:

H2. Perceived severity of sanction has a more significant effect on behavioural intention towards smartphone security behaviour among female employees than male employees.

4.3 Perceived risk vulnerability

Perceived risk vulnerability refers to the individual's perception of the risk associated with the use of information security (van Schaik et al., 2017). It also refers to the probability that the risk is realised by an individual. Previous studies showed that there is a strong relationship between perceived risk and precautionary behaviour (Siponen et al., 2006; Van Der Pligt, 1998). In addition, previous studies showed that females are less aware of and more concerned with security threats than males (Johnson & Koch, 2006). Hence, female employees can be particularly vulnerable to security breaches emanating from a lack of awareness of the risk associated with the unsafe use of smartphones. Therefore, we propose the following hypothesis:

H3. Perceived risk vulnerability has a more significant effect on behavioural intention towards smartphone security behaviour among female employees than male employees.

4.4 Response cost

Response cost refers to the perceived costs incurred by a user in performing a recommended coping behaviour (Chenoweth, Minch, & Gattiker, 2009). This factor may include monetary expense, inconvenience, difficulty and the side effects of performing the coping behaviour (Helmes, 2002). It was found significant in previous studies (Helmes, 2002; Neuwirth, Dunwoody, & Griffin, 2000). Previous studies showed that females struggle more than males with the use of technology when they encounter difficulties (Venkatesh, Thong, & Xu, 2012). Hence, response cost may be more significant among females than males. Therefore, we propose the following hypothesis:

H4. Response cost has a more significant effect on behavioural intention towards smartphone security behaviour among female employees than male employees.

4.5 Perceived certainty of sanction

Perceived certainty of sanction refers to the individual's level of certainty of a formal sanction as a result of the misuse of information systems (D'Arcy & Herath, 2011; Willison et al., 2018). This factor is one of the classic GDT factors which explains that the higher the level of certainty of sanction, the more individuals will be deterred from any unsafe behaviour (Gibbs, 1975). Herath and Rao (2009a; 2009b) found a positive relationship

Journal Pre-proof

between individuals' certainty of sanction and information systems security intention. Certainty of sanction is related to strong moral commitment among employees (D'Arcy & Herath, 2011). Previous studies showed that women have stronger perceptions of sanction certainty than men do, and they have lower levels of participation rates in crime than men (Carmichael, 2004; Gavrilova & Campaniello, 2015). Because women are less likely to be involved in committing crimes, they have a stronger moral commitment and a higher perceived certainty of sanction (Gavrilova & Campaniello, 2015; Paternoster, Saltzman, Waldo, & Chiricos, 1985). Therefore, this factor may have a more significant effect among female employees than male employees, as indicated in previous research conducted by Carmichael (2004). Thus, we propose the following hypothesis:

H5. Perceived certainty of sanction has a more significant effect on behavioural intention towards smartphone security behaviour among female employees than male employees.

4.6 Severity of adverse consequences

Severity of adverse consequences refers to the consequences (in terms of security threats to the organisation) which may arise from not following the organisation's information security recommendations (Ifinedo, 2012). This factor tends to have a positive relationship with cybersecurity intentions among employees (Bulgurcu et al., 2010). This can also be applicable to the case of smartphone security. The severity of adverse consequences is often linked to awareness of the types and severity of security threats that the organisation can face (Öğütçü, Testik, & Chouseinoglou, 2016). Previous studies showed that this factor has a more significant effect among female employees (Anwar et al., 2017). Thus, we propose the following hypothesis:

H6. Perceived severity of adverse consequences has a more significant effect on behavioural intention towards smartphone security behaviour among female employees than male employees.

4.7 Response efficacy

Response efficacy is the degree to which a person believes that the recommended response will be effective (Boss, Galletta, Lowry, Moody, & Polak, 2015; Maddux & Rogers, 1983). It has a significant effect on protection motivation (Boss et al., 2015; Vance et al., 2012). It refers to employees' beliefs that following with information security recommendations would help to keep any security breaches limited (Vance et al., 2012). The study conducted by Anwar et al. (2017) showed that there are no significant differences between males and females in terms of the significance of response efficacy. Thus, we propose the following hypothesis:

H7. Response efficacy has a significant effect on behavioural intention towards smartphone security behaviour among both male and female employees than male employees.

4.8 Uncertainty avoidance

Uncertainty avoidance refers to the way that a society deals with the fact that the future can never be known (Hofstede, 2019). It links to the ambiguity of the future which can bring anxiety to humans (Björck, 2006). Within the context of employee smartphone security behaviour, this factor can play an important role, as employees who have higher uncertainty avoidance espoused national cultural values may have a high level of fear of what may happen as a consequence of smartphone misuse. Companies develop detailed systems, rules

Journal Pre-proof

and procedures (Stedham & Yamamura, 2002). Previous studies showed that women tend to be more intuitive than men in terms of decision making (Moskites, 2017). However, when women are put in a situation that can lead to a cybersecurity threat, they tend to be more analytical and data-driven in their decision making than men (Moskites, 2017). Hence, when a situation involves uncertainty and insufficient information is provided, female employees might be more affected than male employees. Thus, uncertainty avoidance may have a stronger effect on intention towards smartphone security behaviour among female employees. Thus, we propose the following hypothesis:

H8a. Uncertainty avoidance has a more significant effect on behavioural intention towards smartphone security behaviour among female employees than male employees.

4.9 Power distance

Power distance refers to the equal distribution of power across individuals in the society (Hofstede, 2019). A society with a high level of power distance means that employees in an organisation accept that there is a hierarchal order (Hofstede, 2019). Previous studies showed that women have higher espoused power distance than men (Jahangirov, Saglam Ari, Jahangirov, & Tosunoglu, 2015; Vujovic, Vuckovic, Vujovic & Prostran, 2016). This factor has also been linked to the social influence managers can have on their employees in terms of different decisions related to the use of technology (Khatri, 2009; Sriwindono & Yahya, 2014). Previous studies showed that female employees are more prone to the effects of social influence (Venkatesh, Morris, Davis, & Davis, 2003). Hence, female employees may be more affected by hierarchies in their organisations and they may be more influenced by the views and opinions of their managers as they espouse high power distance cultural values. Thus, we propose the following hypothesis:

H8b. Power distance has a more significant effect on behavioural intention towards smartphone security behaviour among female employees than male employees.

4.10 Individualism vs collectivism

In individualistic societies, individuals are more concerned with themselves and their close circle (Hofstede, 2019). On the other hand, in collectivistic societies, individuals belong to their groups and they are loyal to them (Hofstede, 2019). In other words, individuals in this type of society follow what their groups do. In collectivistic societies employees' behaviour is influenced by the group of employees and the management team (Tarhini et al., 2016). Within the context of BYOD security behaviour, the offence leads to shame and loss of face and the employer-employee relationship is perceived in moral terms (like a family link) (Hofstede, 2019). Hence, employees with espoused collectivist cultural values are expected to be careful with their behaviour and avoid misusing their smartphones that can lead to a threat or an attack to the company's information systems security. Bada, Sasse, and Nurse (2014) indicated that collectivism is crucial for raising awareness and collaboration to ensure information security, because individuals with an espoused collectivist culture tend to work together and have a higher level of awareness of security issues related to their use of technology. Individuals with an espoused collectivist culture tend to define themselves in terms of their relationships and social groups and avoid behaviours that cause social disruption (Triandis, 1989). Women are generally more concerned with connecting to others and maintaining group harmony while men are likely to act independently (Eagly, 1978; Eagly, 1983; Jhangiani & Tarry, 2011). They also tend to espouse collectivist values and are

Journal Pre-proof

less trusting than their male counterparts (Zeffane, 2017). In general, women in both Western and Eastern countries are more collectivistic (Aizawa & Whatley, 2006). This collectivistic nature can lead female employees to have high behavioural intention towards smartphone security. Hence, we propose the following hypothesis:

H8c. Individualism vs collectivism has a more significant effect on behavioural intention towards smartphone security behaviour among female employees than male employees.

4.11 Masculinity vs femininity

In a masculine society, individuals are driven by achievements and success, while in a feminine society, individuals are driving by doing what they like and caring for others (Hofstede, 2019). This factor also refers to the extent to which the traditional gender roles are differentiated (Hofstede, 1980; Tarhini, Hone, & Liu, 2014). It is possible that both masculinity and femininity have an effect on employees' smartphone security behaviour. In a masculine society, individuals are more likely to avoid failure in their job if any security attack occurs due to their actions, which can also impact on their jobs. Men can have a higher status in masculine societies, so they are more likely to be perceived as effective leaders (Jhangiani & Tarry, 2011). Hence, this dimension can have a more significant effect among female employees. In a feminine society, employees follow security procedures as they care for their organisations and other employees since they are more people-oriented. This particular dimension can have a significant effect on female employees and giving female employees their voice in their organisations. Hence, we propose the following hypothesis:

H8d. Masculinity vs femininity has a more significant effect on behavioural intention towards smartphone security behaviour among female employees than male employees.

5. Methodology

5.1 Sampling and data collection

In order to achieve the aim of this research and test the above formulated hypotheses, a total of 1300 questionnaires were distributed to employees (aged 18–35) in international companies in both the US (Boston) and the UAE (Dubai). A total of 650 questionnaires were distributed face to face in both countries. This particular age group of employees is more active in using BYOD (Aruba Networks, 2014).

This research employed purposive sampling to target the specific age group of participants. This sampling method is useful when the process of recruiting participants in the research is based on selecting individuals with similar characteristics (Etikan, Mus, & Alkassim, 2016). In other words, it is based on the judgement of the researcher. This method allowed the selection of participants in the specific age group targeted in this research. The questionnaire was distributed in English in both countries, because English is widely used in the UAE (Eid & Elbanna, 2017). A total of 554 completed questionnaires from the UAE and 602 questionnaires from the US were included in the analysis. The response rate was 93% in the US and 85% in the UAE, which indicates a high response rate. The questionnaires were self-administered, which helped to achieve these high response rates (Couper, 2005; Lam, Cho, & Qu, 2007).

5.2 Measurements

This research used a seven-point Likert scale, ranging from 1 – strongly disagree to 7– strongly agree for the items of the factors included in our proposed model, following what

Journal Pre-proof

has been adopted in previous studies (Venkatesh et al., 2003). We adopted most measurement items from previously tested measures in previous studies to increase their validity: four items for behavioural intention (BI) adopted from Herath and Rao's (2009a) study, five items for masculinity vs femininity (MF) adopted from Srite and Karahanna's (2006) study, six items for individualism vs collectivism (IC) adopted from Srite and Karahanna's (2006), seven items for power distance (PD) adopted from Srite and Karahanna's (2006) study, six items for uncertainty avoidance (UA) adopted from Srite and Karahanna's (2006), three items for self-efficacy (SE) adopted from Herath and Rao's (2009a), six items for response efficacy (RE) adopted from Vance et al.'s (2012) study, six items for response cost (RC) adopted from Vance et al.'s (2012) study, two items for severity of adverse consequences (SAC) adopted from Ifinedo's (2016) study (with minor modifications), two items for perceived certainty of sanction (PCS) adopted from the studies conducted by Graham Peace, Galletta, and Thong, (2003), Herath and Rao, (2009a) and Knapp, Marshall, Rainer, and Ford (2005), three items for perceived risk vulnerability (PV) adopted from Putri and Hovav's (2014) study, three items for perceived severity of sanction (PSS) adopted from the studies conducted by Herath and Rao (2009a), Graham Peace et al., (2003) and Knapp et al. (2005) studies. Appendix A shows the items of each factor and their sources.

5.3 Data analysis

The initial stage of the analysis was the data screening using Statistical Package for the Social Sciences (SPSS) version 24. Data was assessed in terms of missing values, outliers and normality issues (Hair et al., 2017; Kline, 2005). Researchers assume that values greater than 3.0 indicate that the data is extremely skewed (Kline, 2005). The normality assessment using skewness and kurtosis values showed that the data in both countries is not normally distributed (Hair, Sarstedt, Hopkins, & Kuppelwieser, 2014).

The second stage of the analysis was analysing the data using partial least squares-structural equation modelling (PLS-SEM) (Hair et al., 2014; Hair et al., 2017; Hair, Black, & Babin, 2019; Hair, Sarstedt, & Ringle, 2019). This method of data analysis includes two stages. First, the assessment of the measurement model. Second, the assessment of the structural model. We used partial least squares-multi-group analysis (PLS-MGA) (Henseler, Ringle, & Sinkovics, 2009) and used gender as a moderator in the model. The analysis was conducted using Smart PLS software (v3.2.7). The PLS analysis was to conduct the partial least squares multi-group analysis (PLS-MGA). *P* values of 0.05 or lower or 0.95 or higher indicate that there are significant differences between the paths in the groups (Henseler et al., 2009). The sample from each country was analysed separately.

6. Results

6.1 Descriptive statistics

For the US sample, the results show that 49% of the respondents were in the 18–22 age group and 51% of them were in the 23–35 age group. 42% of them were male and 58% were female. 55% of the respondents were aware of their organisations' BYOD smartphone security policies, while 45% were not aware of them. The respondents worked in the following industries: finance (15%), transport (15%), construction (14%), automotive (13%), health (11%), manufacturing (11%), education (9%), utilities (7%), and media (4%). Five respondents did not indicate the industry they worked in. All respondents in the US used their personal smartphones for work purposes. For the UAE sample, the results show that 41% of

Journal Pre-proof

the respondents were in the 18–22 age group, while 59% of them were in the 23–35 age group; 79% of the respondents were male and 21% were female; 26% of the respondents indicated that they were aware of their organisations' BYOD policies in the UAE, while 74% indicated that they were not aware of any of these policies. The respondents worked in the following industries: finance (34%), utilities (25%), automotive (24%), education (11%), and media (4%). All respondents indicated that they used their personal smartphones for work purposes.

6.2 Measurement model

The first stage of the PLS analysis was assessing the measurement model for each sample. The assessment of the measurement model was conducted by assessing the validity and reliability of the data. The reliability of the data was assessed using Cronbach's alpha and composite reliability (Hair et al., 2017). No issues in either sample were identified as all values were above the threshold value of 0.7 for both Cronbach's alpha and composite reliability (Hair et al., 2017). In addition, we assessed the convergent validity and discriminant validity of the data. The average variance extracted (AVE) values in both samples and all values were above the threshold value of 0.5 (Hair et al., 2017). In the UAE sample, the Cronbach's alpha values ranged from 0.658 (nearly 0.7) to 0.889. In the USA sample, the Cronbach's alpha values ranged from 0.701 (nearly 0.7) to 0.898. The composite reliability values for the UAE sample ranged from 0.681 to 0.901, while for the USA, the composite reliability ranged from 0.671 (nearly 0.7) to 0.894. As for the AVE values, they ranged from 0.551 to 0.981 in the UAE sample and from 0.654 to 0.938 in the USA sample.

We also assessed the factor loadings in both samples. Some of the items did not have sufficient loadings, as they were below the threshold of 0.5 (Hair et al., 2017), so they were removed including IC4, PD4, UA6, RC3 and RC5 (as shown in Appendix A). The remaining factor loadings for the UAE sample ranged from 0.641 to 0.965, while the remaining factor loadings for the US sample ranged from 0.578 to 0.993. We also assessed the discriminant validity using cross loadings and Fornell-Larcker criterion and the results showed that the constructs share more variance with their own indicators than they share with the indicators of the other constructs, so there were no issues (Hair et al., 2017).

In addition, collinearity was assessed using the variance inflation factor (VIF), with a threshold value of 5 (Hair et al., 2014). The results showed that no major issues exist as all VIF values were lower than the threshold value of 5 in both samples. The highest VIF value in the UAE sample is 2.874 and in the US sample, 3.471. We also assessed multicollinearity using the VIF values. All VIF inner values were lower than 5 for the two samples.

6.3 Multigroup analysis

The second stage of the analysis was conducting the PLS-MGA test for both samples. The samples were separated based on gender distribution (79% of the respondents were male and 21% were female in the UAE sample and 42% were male and 58% were female in the US sample). PLS-MGA is able to handle small and different sample sizes, which makes it appropriate for the analysis of the data collected in this research (Hair et al., 2014; Hair et al., 2017; Henseler et al., 2009). The PLS-MGA test relies on assessing the observed distribution of the bootstrap outcomes instead of making distributional assumptions (Henseler et al., 2009). First, the centred bootstrap estimates of the groups are compared. Then the difference between the groups is divided by the total number of bootstrap samples. This calculates the probability that the significance in the second group is greater than the significance in the

Journal Pre-proof

first group. The difference is evaluated using the *p* value (Henseler et al., 2009). Tables 4 and 5 show the results of the PLS-MGA for both samples.

Journal Pre-proof

Journal Pre-proof

Table 4. Results of PLS-MGA in the UAE sample

Hypothesis	Relationship	*p*-value (group diff)	Mean (males)	Standard deviation (males)	*t*-value (males)	*p*-value (males)	Mean (females)	Standard deviation (females)	*t*-value (females)	*p*-value (females)	Result
H1	SE → INT	0.601	4.21	1.14	0.440	0.456	4.38	1.00	0.986	0.419	Not supported
H2	PSS → INT	0.027	4.86	1.34	1.984	0.031	4.21	1.04	0.028	0.174	Partially supported
H3	PV → INT	0.349	3.20	1.20	1.846	0.081	3.18	1.32	1.962	0.059	Not supported
H4	RC → INT	0.654	3.21	1.00	0.042	0.981	3.46	1.22	0.265	0.971	Not supported
H5	PCS → INT	0.997	5.56	1.06	7.538	0.000	5.28	1.28	6.542	0.000	Supported
H6	SAC → INT	0.971	4.93	1.02	6.429	0.000	5.21	1.10	7.985	0.000	Supported
H7	RE → INT	0.224	3.12	1.27	1.791	0.075	3.18	1.18	0.781	0.573	Not supported
H8a	UA → INT	0.031	4.32	1.22	1.981	0.046	5.98	1.28	1.457	0.198	Partially supported
H8b	PD → INT	0.009	5.78	1.17	2.655	0.009	4.21	1.00	0.823	0.498	Partially supported
H8c	IC → INT	0.004	5.67	1.10	2.451	0.025	4.28	0.95	0.438	0.986	Partially supported
H8d	MF → INT	0.988	5.10	1.00	1.986	0.000	5.47	1.04	4.007	0.000	Supported

Journal Pre-proof

Journal Pre-proof

For the UAE sample, the results showed H5 (PCS → INT, p = .997), H6 (SAC → INT, p = .971) and H8d (MF → INT, p = .988) are supported, while H2 (PSS → INT, p = .027), H8a (UA → INT, p = .031), H8b (PD → INT, p = .009) and H8c (IC → INT, p = .004) are partially supported as there were significant differences between the groups but in the opposite direction to what was hypothesised. The remaining hypotheses were not supported.

Journal Pre-proof

Journal Pre-proof

Table 5. Results of PLS-MGA in the US sample

Hypothesis	Relationship	p-value (group diff)	Mean (males)	Standard deviation (males)	t-value (males)	p-value (males)	Mean (females)	Standard deviation (females)	t-value (females)	p-value (females)	Results
H1	SE → INT	0.958	5.37	1.31	0.079	0.948	5.66	1.27	2.549	0.026	Partially supported
H2	PSS → INT	0.383	4.86	1.34	1.872	0.071	4.45	1.13	1.009	0.425	Not supported
H3	PV → INT	0.791	3.45	1.30	0.418	0.842	3.16	0.95	1.285	0.349	Not supported
H4	RC → INT	0.968	4.96	1.17	0.891	0.651	5.66	1.27	3.949	0.000	Supported
H5	PCS → INT	0.581	5.93	1.02	2.315	0.031	5.40	1.00	2.069	0.028	Not supported
H6	SAC → INT	0.981	4.67	1.11	0.623	0.723	5.26	1.06	2.479	0.038	Supported
H7	RE → INT	0.863	4.17	1.09	0.964	0.512	3.20	1.02	1.581	0.163	Not supported
H8a	UA → INT	0.991	3.25	1.28	0.581	0.746	5.71	1.13	2.808	0.009	Supported
H8b	PD → INT	0.029	5.78	1.05	3.925	0.000	4.31	1.32	1.669	0.123	Partially supported
H8c	IC → INT	0.303	5.26	1.06	4.349	0.000	5.48	1.13	2.851	0.009	Not supported
H8d	MF → INT	0.994	5.18	1.21	1.991	0.000	5.72	1.10	2.768	0.043	Supported

Journal Pre-proof

Journal Pre-proof

For the US sample, H4 (RC → INT, p = .968), H6 (SAC → INT, p = .981), H8a (UA → INT, p = .991) and H8d (MF → INT, p = .994) were supported, while H1 (SE → INT, p = .958) and H8b (PD → INT, p = .029) were partially supported as there were significant differences between the groups but in the opposite direction to what we hypothesised. The remaining hypotheses were not supported.

7. Discussion

This study analysed gender differences in terms of the factors that can affect employees' security behavioural intention when using personal smartphones for work-related activities in a cross-national/cultural context, namely, in the US and UAE. Our literature review showed that research on gender differences in employees' cybersecurity behaviour is scarce. However, our findings reveal that there are significant gender differences in smartphone security behavioural intention among employees in international companies whether in an advanced country in terms of cybersecurity defence or a country which is considered behind in this area. There are significant gender differences in both the US and the UAE in terms of punishment severity and certainty. In addition, there are significant gender differences among employees in both countries in terms of the effects of their espoused national cultural values on BYOD security behavioural intention. We found that the effects of espoused national cultural values are different in the context of BYOD security behavioural intention. Female employees in both countries are more affected by the nature of the culture around them, whether it is a masculine or a feminine society.

The results showed that self-efficacy (H1) has an insignificant effect among both males and females in the UAE. However, this factor has a significant effect on behavioural intention of females in the US, which contradicts with our hypothesis. This shows that female employees in the US find self-confidence in undertaking the steps required to ensure the security of their smartphones as an important factor, which is consistent with the findings of He and Freeman (2010) and Latikka et al. (2019). This is linked to the knowledge ad awareness of the recommended security behaviour.

Contrary to what we hypothesised, perceived severity of sanction (H2) has a more significant effect on behavioural intention among males than females in the UAE. This contradicts with the findings of previous studies on gender differences in criminology (Callanan & Teasdale, 2009; Hale, 1996). In addition, this factor has an insignificant effect on behavioural intention among both males and females in the US. This indicates a lack of awareness of the type of punishment that can occur as a result of a breach of security caused by employees, both male and female employees, misusing their smartphones in the US.

We found that perceived risk vulnerability has no significant effect on behavioural intention (H3) among males or females in either the US or UAE. This contradicts with the findings of previous studies (e.g. Siponen et al., 2006). It indicates a general lack of awareness among both male and female employees in both countries of the risks associated with their use of smartphones in terms of security issues. This may also indicate a lack of employee awareness programmes on the risks associated with misusing smartphones.

Although the findings revealed that response cost does not have a significant effect of behavioural intention towards smartphone security behaviour (H4) among male or female

Journal Pre-proof

employees in the UAE, this factor is significant among female employees in the US. The findings in the US support the findings of Helmes (2002), Neuwirth et al. (2000) and Li et al. (2019). This shows that female employees in the US are more aware of the difficulties (cost) associated with keeping their smartphones secure.

The analysis of the data supported our hypothesis that perceived certainty of sanction has a more significant effect on behavioural intention towards smartphone security behaviour (H5) among females in the UAE but not in the US. Thus, this supports the findings in Carmichael's (2004) study as the author reported the significance of this factor. Nevertheless, the findings also revealed that this factor is significant among both male and female employees in both countries. This indicates that employees in both countries are aware of the certainty of the punishment of their actions translated in the form of certainty of formal sanctions, even though they may not be fully aware of the risks and the type of punishment they may face.

Perceived severity of adverse consequences has a more significant effect on behavioural intention towards smartphone security behaviour (H6) among female employees in both countries, thus providing support to our hypothesis and the study conducted by Anwar et al. (2017). Female employees' awareness of the security threats/attacks their organisations may face as a result of any unsafe behaviour that does not follow their organisations' security recommendations is an important predictor of their smartphone security behaviour.

Surprisingly, the results show that response efficacy is not significant among both male and female employees (H7) in both the UAE and the US. This contradicts the findings of many previous studies (e.g. Anwar et al., 2017; Boss et al., 2015; Vance et al., 2012) as they reported the significance of this factor. This indicates that both male and female employees in both countries do not perceive the current organisational security policies and recommendations in their organisations as present and effective to have a significant effect on their behavioural intention towards smartphone security.

In terms of the effects of employees' espoused national cultural values, the results of the data analysis from both samples are contradicting. Overall, the findings show significant differences between male and female employees in terms of how their espoused national cultural values affect their BYOD (smartphone) security behaviour. While the effect of employees' espoused uncertainty avoidance has a stronger effect on intention towards smartphone security behaviour (H8a) among Emirati male employees, it has a more significant effect among female employees in the US. This is also associated with how they view rules and procedures (Stedham & Yamamura, 2002). Male employees in the UAE and female employees in the US view uncertainty avoidance as an important factor and pay more attention to rules and procedures for ensuring smartphone security. They feel the need to have the knowledge necessary to avoid the uncertainties associated with their smartphone security behaviour.

The data analysis revealed some surprising findings on power distance. While we hypothesised that employees' espoused power distance would have a more significant effect on intention towards smartphone security behaviour (H8b) among female employees due to its link to social influence, the results revealed that espoused power distance had a more significant effect on intention among male employees in both countries. This contradicts with the findings of Venkatesh et al. (2003), as it shows that the influence and power of the

Journal Pre-proof

management has a more significant effect on smartphone security behaviour among male employees.

Contrary to our hypothesis, individuals' espoused individualism vs collectivism has a more significant effect on behavioural intention (H8c) among male employees in the UAE. In addition, no significant differences were found between male and female employees in the US, as individuals' espoused individualism vs collectivism has a significant effect on behavioural intention among both male and female employees but has a slightly higher effect among male employees. The results contradict with the findings of previous studies on the differences between men and women in terms of how they interact with certain groups. Male employees tend to be more affected by the type of society they are. Male employees in the UAE are more likely to be affected by their type of society (individualistic or collectivistic) to take the correct action in terms of smartphone security. This is also the case for both male and female employees in the US.

The findings supported our hypothesis that employees' espoused masculinity vs femininity has a more significant effect on behavioural intention towards smartphone security behaviour (H8d) among female employees in both countries. This shows that female employees' smartphone security behaviour is affected by whether a society is perceived as masculine or feminine as it affects the role they play in ensuring the security of their organisations' systems and data on their smartphones. This means that the possibility of recognition of women's achievements in terms of keeping their devices secure is an important factor for them.

8. Contributions and future work

8.1 Theoretical contributions

This study contributes to the existing body of literature in three main ways. First, the study focused on a relatively new area of research, gender differences in smartphone security behavioural intention among employees in international companies. Second, this is the first study to account for the role of employees' espoused national cultural values (Hofstede's cultural dimensions) while proposing a new model, the BMS, which combines the PMT and the GDT. The inclusion of Hofstede's cultural dimensions (namely, power distance, uncertainty avoidance, femininity vs masculinity and individualism vs collectivism) is especially important when taking employees gender differences in BYOD security behavioural intention into account. Third, the comparison of the results of the data collection from two countries (UAE and US) is another important contribution as it allowed our proposed model, the BMS, to be tested in two countries that are ranked differently in terms of the cybersecurity index.

8.2 Practical implications

Our results have a number of practical implications for business and policymakers in the US and the UAE. The findings of our research show that employees (both male and female employees and in both countries) are not aware of the risks associated with their use of smartphones. In addition, there is a lack of employees' awareness of their organisations' smartphone security policies and the level of threat they can face in the case of not following their organisations' security requirements. Furthermore, employees in both countries do not believe that the behaviour recommended by their organisations is effective in ensuring the security of BYODs and increasing their smartphone security behavioural intention (response

Journal Pre-proof

efficacy) for smartphone security. Hence, it is recommended that organisations use a more open approach in developing their BYOD security policies and recommended behaviour in which employees' voices and views are taken into consideration.

Understanding employees' espoused national cultural values in terms of the four dimensions this study has focused on is an important area for managers to focus on. This will help managers to understand the external influences on their employees' smartphone security behavioural intention, taking into account the significant differences between male and female employees in terms of their espoused national cultural values. Since female employees in both countries are less influenced by the hierarchies in their organisations and the influence of managers, other forms of persuasion could be used, such as acknowledging their achievements in keeping their smartphones secure.

Female employees in the UAE need to be made aware of the severity of the punishments that can occur as a result of non-secure behaviour. Surprisingly, this is also the case for both male and female employees in the US. Hence, there is a need for making employees (female employees in the UAE and both male and female employees in the US) aware of the types of punishments and disciplinary actions that can take place if they do not follow with their organisations' BYOD security recommendations. Female employees in the US consider the difficulties associated with following their organisations' BYOD security recommendations as an important factor. Hence, companies in the US are recommended to provide further training to their female employees to reduce the difficulties associated with following with their BYOD security recommendations. Our results show that female employees in both countries have a higher level of awareness of the types and severity of security threats that the organisation can face than male employees. Hence, security awareness campaigns to raise male employees' awareness of the significance of BYOD security in their companies will be beneficial.

8.3 Limitations and future research directions

The findings of this research are limited to a specific age group of employees (18–35 years old) who are categorised as the gen-mobile workforce due to their ability in providing an informed view of the security of smartphones for work. However, future research can focus on other, more specifically older age groups and compare the findings with the findings of our research. In addition, our research focused on two countries which are different in terms of their cybersecurity defence level, but they are both considered advanced in comparison to other, developing countries. Future research can collect data from other less-developed countries in a cross-national context while focusing on female employees who usually suffer from economic, social and legal rights in these countries and they are less informed of the security issues associated with the use of smartphones for work in comparison to the female employees included in our sample. Furthermore, our research highlighted important findings regarding the lack of employees' awareness of their organisations' smartphone security policies and procedures. It focused on collecting data from employees in various companies to test their BYOD (smartphone) security behavioural intention. Nevertheless, some of the participants indicated that they were unaware of their companies' smartphone security policies. Hence, some of the responses may have been hypothetical. Future studies can collect data from specific companies rather than employees in general and collect data on the targeted companies' information security policies prior to distributing questionnaires to employees working in these companies.

Journal Pre-proof

9. Conclusion

This research sought to examine gender differences in BYOD (smartphone) security behavioural intention among employees in both the UAE and US in order to bridge the gap in research in this area. Given that BYOD security is becoming a major problem and that the number of female employees in the workforce is increasing worldwide, understanding gender differences in a cross-national context is an important and timely subject. The study revealed that both male and female employees in both countries do not perceive their organisations' recommendations and policies as present and effective to have a significant effect on their behavioural intention towards smartphone security behaviour. In addition, both male and female employees may not be fully aware of the security-related risks associated with using their smartphones for work and personal purposes. Furthermore, employees' espoused national cultural values play a significant role in their smartphone security behavioural intention in both countries, with some gender differences identified in this area. The identification and understanding of these differences help to reduce the threats associated with the use of BYOD among employees securely and acknowledging women's voice in this process. Indeed, the growing business relationships between both countries necessitates the cross-national investigation, which would ultimately help bridge any real or perceived cultural constraints in the workplace.

Appendix A. Items for each construct and their sources

Factor/items	Source
Behavioural intention (BI)	Herath and Rao (2009a)
INT1: I intend to follow the smartphone security policies and practices for using smartphones at work.	
INT2: I intend to use the smartphone security technologies for using smartphones at work.	
INT3: I intend to use common sense on good smartphone security practices for using smartphones at work.	
Masculinity vs femininity (MF)	Srite and Karahanna (2006)
MF1: It is preferable to have a man in high level position rather than a woman.	
MF2: There are some jobs in which a man can always do better than a woman.	
MF3: It is more important for men to have a professional career than it is for women to have a professional career.	
MF4: Solving organisational problems requires the active forcible approach which is typical of men.	
MF5: Women do not value recognition and promotion in their work as much as men do.	
Individualism vs collectivism (IC)	Srite and Karahanna (2006)
IC1: Being accepted as a member of a group is more important than having autonomy and independence.	
IC2: Being accepted as a member of a group is more important than being independent.	
IC3: Group success is more important than individual success.	
IC4: Being loyal to a group is more important than individual gain.	(Dropped, USA sample)
IC5: Individual rewards are not as important as group welfare.	

Journal Pre-proof

IC6: It is more important for a manager to encourage loyalty and a sense of duty in subordinates than it is to encourage individual initiative.	
Power distance (PD)	Srite and Karahanna (2006)
PD1: Managers should make most decisions without consulting subordinates.	
PD2: Managers should not ask subordinates for advice, because they might appear less powerful.	
PD3: Decision making power should stay with top management in the organisation and not be delegated to lower level employees.	
PD4: Employees should not question their manager's decisions.	(Dropped, UAE sample)
PD5: A manager should perform work which is difficult and important and delegate tasks which are repetitive and mundane to subordinates.	
PD6: Higher level managers should receive more benefits and privileges than lower level managers and professional staff.	
PD7: Managers should be careful not to ask the opinions of subordinates too frequently, otherwise the manager might appear to be weak and incompetent.	
Uncertainty avoidance (UA)	Srite and Karahanna (2006)
UA1: Rules and regulations are important because they inform workers what the organisation expects of them.	
UA2: Order and structure are very important in a work environment.	
UA3: It is important to have job requirements and instructions spelled out in detail so that people always know what they are expected to do.	
UA4: It is better to have a bad situation that you know about, than to have an uncertain situation which might be better.	
UA5: Providing opportunities to be innovative is more important than requiring standardised work procedures.	
UA6: People should avoid making changes because things could get worse.	(Dropped, UAE sample)
Self-efficacy (SE)	Herath and Rao (2009a)
SE1: I would feel comfortable following most of the smartphone security policies on my own.	
SE2: If I wanted to, I could easily follow smartphone security policies on my own.	
SE3: I would be able to follow most of the smartphone security policies even if there was no one around to help me.	
Response efficacy (RE)	Vance et al. (2012)
RE1: Complying with smartphone security policy reduces the security threat to my organisation's information.	
RE2: Complying with smartphone security policy reduces the security threat to my personal data.	
RE3: If I comply with smartphone security policy, mobile security problems in my organisation will be scarce.	
RE4: If I comply with smartphone security policy, my mobile device related security problems will be scarce.	
RE5: Compliance with smartphone security policy would help to reduce IS security problems in my organisation.	
RE6: Compliance with smartphone security policy would help me reduce security problems with my own personal data.	

Journal Pre-proof

Response cost (RC)	Vance et al. (2012)
RC1: Complying with smartphone security policy would interfere with my work.	
RC2: Complying with smartphone security policy would interfere with the personal use on my device.	
RC3: There are too many overheads associated with complying with smartphone security policies.	(Dropped, USA sample)
RC4: Complying with smartphone security policy would require considerable investment of effort other than time.	
RC5: Complying with smartphone security policy would take considerable amount of my working time.	(Dropped, UAE sample)
RC6: Complying with smartphone security policy would take considerable amount of my personal time.	
Severity of adverse consequences (SAC)	Ifinedo (2016) (with minor modifications)
SAC1: Employee mobile practices are properly monitored for policy violations.	
SAC2: If I violate organisation BYOD security policies, I would probably be caught.	
Perceived certainty of sanction (PCS)	Graham Peace, Galletta, and Thong (2003), Herath and Rao (2009a), Knapp, Marshall, Rainer, and Ford (2005)
PCS1: Employee computer practices are properly monitored for policy violations.	
PCS2: If I violate organisation security policies, I would probably be caught.	
Perceived risk vulnerability (PV)	Putri and Hovav (2014)
PV1: I could be subjected to an information security threat, if I don't comply with the organisation's smartphone security policy.	
PV2: A security problem to my organisation's information could occur if I don't comply with the organisation's smartphone security policy.	
PV3: A security problem to my personal data could occur if I don't comply with the organisation's smartphone security policy.	
Perceived severity of sanction (PSS)	Herath and Rao (2009a), Graham Peace et al., (2003), Knapp et al. (2005)
PSS1: The organisation disciplines employees who break information security rules.	
PSS2: My organisation terminates employees who repeatedly break security rules.	
PSS3: If I were caught violating organisation information security policies, I would be severely punished.	

Journal Pre-proof

Journal Pre-proof

References

Aizawa, Y., & Whatley, M. A., (2006). Gender, shyness, and individualism-collectivism: A cross-cultural study. *Race, Gender & Class, 13*(2), 7–25.

Akman, I., & Mishra, A. (2010). Gender, age and income differences in internet usage among employees in organisations. *Computers in Human Behavior, 26*(3), 482–490.

Alaskar, M., & Shen, K. N. (2016). Understanding bring your own device (BYOD) and employee information security behaviors from a work-life domain perspective. Proceedings of 22nd Americas Conference on Information Systems.

Alshare, K. A., Lane, P. L., & Lane, M. R. (2018). Information security policy compliance: A higher education case study. *Information & Computer Security*, *26*(1), 91–108.

Ameen, N., & Willis, R. (2018a). Towards a generalized model for smartphone adoption and use in an Arab context: A cross-country comparison. *Information Systems Management, 35*(3), 254–274.

Ameen, N., & Willis, R. (2018b). Towards closing the gender gap in Iraq: Understanding gender differences in smartphone adoption and use. *Information Technology for Development*, 1–26. https://doi.org/10.1080/02681102.2018.1454877.

Ameen, N., Willis, R., & Shah, M. H. (2018). An examination of the gender gap in smartphone adoption and use in Arab countries: A cross-national study. *Computers in Human Behavior, 89*, 148–162.

Anderson, C. L., & Agarwal, R. (2010). Practicing safe computing: A multimedia empirical examination of home computer user security behavioral intentions. *MIS Quarterly, 34*(3), 613–643

Anwar, M., He, W., Ash, I., Yuan, X., Li, L., & Xu, L. (2017). Gender difference and employees' cybersecurity behaviors. *Computers in Human Behavior, 69*, 437–443.

Arpaci, I. (2019). A theoretical framework for IT consumerization: Factors influencing the adoption of BYOD. In C. Idemudia, C. (Ed.), *Handbook of research on technology integration in the global world* (pp. 114–129). Arkansas Tech University, USA: IGI Global.

Aruba Networks. (2014). *Are you ready for the gen-mobile?* https://www.arubanetworks.com/pdf/solutions/GenMobile_Report.pdf Accessed 28 March 2019.

Bada, M., Sasse, A.M. & Nurse, J.R., (2014). Cyber Security Awareness Campaigns: Why do they fail to change behaviour?. *Cryptography and Security*, Doi: arXiv:1901.02672.

Badam, R. (2018, July 27). Numbers of working women in UAE surge, report reveals. *The National*. https://www.thenational.ae/uae/government/numbers-of-working-women-in-uae-surge-report-reveals-1.737024 Accessed 16 March 2019.

Baillette, P., Barlette, Y., & Leclercq-Vandelannoitte, A. (2018). Bring your own device in organisations: Extending the reversed IT adoption logic to security paradoxes for CEOs and end users. *International Journal of Information Management, 43*, 76–84.

Bautista, J. R., Rosenthal, S., Lin, T. T., & Theng, Y. L. (2018). Predictors and outcomes of nurses' use of smartphones for work purposes. *Computers in Human Behavior, 84*, 360–374.

Journal Pre-proof

Bhandari, A. (2019). Gender inequality in mobile technology access: The role of economic and social development. *Information, Communication & Society, 22*(5), 1–17. https://doi.org/10.1080/1369118X.2018.1563206.

Björck, J., & Jiang, K. (2006). *Information security and national culture* (MSc thesis). KTH Royal Institute of Technology, Stockholm, Sweden.

Blythe, J. M., & Coventry, L. (2018). Costly but effective: Comparing the factors that influence employee anti-malware behaviours. *Computers in Human Behavior, 87*, 87–97.

Boss, S., Galletta, D., Lowry, P. B., Moody, G. D., & Polak, P. (2015). What do systems users have to fear? Using fear appeals to engender threats and fear that motivate protective security behaviors. *MIS Quarterly, 39*(4), 837–864.

Brown, W. S., & Palvia, P. (2015). Are mobile devices threatening your work-life balance? *International Journal of Mobile Communications, 13*(3), 317–338.

Bulgurcu, B., Cavusoglu, H., & Benbasat, I. (2010). Information security policy compliance: An empirical study of rationality-based beliefs and information security awareness. *MIS Quarterly, 34*(3), 523–548.

Buller, A. (2018, January 10). UAE tech growth prompts firms to review internal IT security. *Computer Weekly*. https://www.computerweekly.com/news/450432909/UAE-tech-growth-prompts-firms-to-review-internal-IT-security Accessed 16 March 2019.

Bullock, L. (2019, January 21). The future of BYOD: Statistics, predictions and best practices to prep for the future. *Forbes*. https://www.forbes.com/sites/lilachbullock/2019/01/21/the-future-of-byod-statistics-predictions-and-best-practices-to-prep-for-the-future/#254b81281f30 Accessed 28 March 2019.

Callanan, V. J., & Teasdale, B. (2009). An exploration of gender differences in measurement of fear of crime. *Feminist Criminology, 4*(4), 359–376.

Carmichael, S. E. (2004). *Gender differences and perceived sanction threats: The effect of arrest ratios* (Doctoral dissertation). University of Florida.

Chen, X., Wu, D., Chen, L., & Teng, J. K. (2018). Sanction severity and employees' information security policy compliance: Investigating mediating, moderating, and control variables. *Information & Management, 55*(8), 1049–1060.

Cheng, L., Li, Y., Li, W., Holm, E., & Zhai, Q. (2013). Understanding the violation of IS security policy in organisations: An integrated model based on social control and deterrence theory. *Computers & Security, 39*(1), 1–13.

Chenoweth, T., Minch, R., & Gattiker, T. (2009). Application of protection motivation theory to adoption of protective technologies. *Proceedings of the 42nd Hawaii International Conference on System Sciences, USA*, 1–10.

Connolly, L. Y., Lang, M., Gathegi, J., & Tygar, D. J. (2017). Organisational culture, procedural countermeasures, and employee security behaviour: A qualitative study. *Information & Computer Security, 25*(2), 118–136.

Couper, M. P. (2005). Technology trends in survey data collection. *Social Science Computer Review, 23*(4), 486–501.

Journal Pre-proof

Crossler, R. E., & Bélanger, F. (2017). The mobile privacy-security knowledge gap model: Understanding behaviors. *Proceedings of the 50th Hawaii International Conference on System Sciences, USA*, 4071–4080.

D'Arcy, J., & Herath, T. (2011). A review and analysis of deterrence theory in the IS security literature: Making sense of the disparate findings. *European Journal of Information Systems, 20*(6), 643–658.

D'Arcy, J., Hovav, A., & Galletta, D. (2009). User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research, 20*(1), 79–98.

Dang-Pham, D., & Pittayachawan, S. (2015). Comparing intention to avoid malware across contexts in a BYOD-enabled Australian university: A protection motivation theory approach. *Computers & Security, 48*, 281–297.

de las Cuevas, P., Mora, A. M., Merelo, J. J., Castillo, P. A., Garcia-Sanchez, P., & Fernandez-Ares, A. (2015). Corporate security solutions for BYOD: A novel user-centric and self-adaptive system. *Computer Communications, 68*, 83–95.

Disterer, G. & Kleiner, C., (2013). BYOD bring your own device. *Procedia Technology*, 9 (1), 43-53.

Doargajudhur, M. S., & Dell, P. (2019). Impact of BYOD on organizational commitment: An empirical investigation. *Information Technology & People, 32*(2), 246–268.

Dubai Government Centre. Dubai statistics: 13.3% of female Emiratis occupy senior positions. (2019). https://www.dsc.gov.ae/en-us/DSC-News/Pages/Emirati-Women-Excel-in-Health-and-Education-Sectors-in-Dubai.aspx Accessed 16 March 2019.

Eagly, A. H. (1978). Sex differences in influenceability. *Psychological Bulletin, 85*, 86–116.

Eagly, A. H. (1983). Gender and social influence: A social psychological analysis. *American Psychologist, 38*, 971–981.

Eid, R., & Elbanna, S. (2017). A triangulation study to assess the perceived city image in the Arab Middle East context: The case of Al-Ain in the UAE. *Tourism Planning & Development, 15*(2), 118–133.

Etikan, I., Mus, S. A., & Alkassim, R. S. (2016). Comparison of convenience sampling and purposive sampling. *American Journal of Theoretical and Applied Statistics, 5*(1), 1–4.

Fetterolf, J. In many countries, at least four-in-ten in the labor force are women. (2018). Pew Research. http://www.pewresearch.org/fact-tank/2017/03/07/in-many-countries-at-least-four-in-ten-in-the-labor-force-are-women/ Accessed 24 March 2019.

Foth, M. (2016). Factors influencing the intention to comply with data protection regulations in hospitals: Based on gender differences in behaviour and deterrence. *European Journal of Information Systems, 25*(2), 91–109.

Gavrilova, E., & Campaniello, N. (2015). *Uncovering the gender participation gap in the crime market*. http://ftp.iza.org/dp8982.pdf Accessed 19 July 2019.

Gibbs, J. P. (1975). *Crime, punishment, and deterrence*. New York: Elsevier.

Journal Pre-proof

Graham Peace, A., Galletta, D. F., & Thong, J. Y. L. (2003). Software piracy in the workplace: A model and empirical test. *Management Information Systems*, *20*(1), 153–177.

Gratian, M., Bandi, S., Cukier, M., Dykstra, J., & Ginther, A. (2018). Correlating human traits and cyber security behavior intentions. *Computers & Security, 73*, 345–358.

Greene, G., & D'Arcy, J. (2010). Assessing the impact of security culture and the employee-organisation relationship on IS security compliance. *Proceedings of the 5th Annual Symposium on Information Assurance (ASIA'10)*, 1-8.

Gregory, M. Navigating collaboration risks and challenges in a BYOD culture. (2018). https://www.neweratech.com/2018/02/07/navigating-collaboration-risks-and-challenges-in-a-byod-culture/ Accessed 24 March 2019.

GSMA. The mobile economy Middle East and North Africa. (2017). https://www.gsmaintelligence.com/research/?file=84935f5774975f3d35c8ed9a41b9c1a4&download Accessed 10 August 2018.

Gulf News (2015, February 2). Defining UAE as world's leading business hub. *Gulf News*. https://gulfnews.com/opinion/editorials/defining-uae-as-world-s-leading-business-hub-1.1450459 Accessed 24 March 2019.

Guo, K. H. (2013). Security-related behavior in using information systems in the workplace: A review and synthesis. *Computers & Security, 32*, 242–251.

Hadlington, L. (2018). The "human factor" in cybersecurity: Exploring the accidental insider. In J. McAlaney, L. A. Frumkin, & V. Benson (Eds.), *Psychological and behavioral examinations in cyber security* (pp. 46–63). Hershey: IGI Global.

Haine, A. (2017, September 21). More women are joining the UAE labour force. *The National*, forcehttps://www.thenational.ae/business/economy/more-women-are-joining-the-uae-labour-force-1.630617 Accessed 24 March 2019.

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). *Multivariate data analysis* (8th ed.).Harlow: Pearson Education.

Hair, J. F., Hult, G. T. M., Ringle, C. M., & Sarstedt, M. (2017). *A primer on partial least squares structural equation modeling*. (2nd ed.). Thousand Oaks, CA: Sage.

Hair J, F., Sarstedt, M., Hopkins, L., & Kuppelwieser, G. V. (2014). Partial least squares structural equation modeling (PLS-SEM): An emerging tool in business research. *European Business Review, 26*(2), 106–121.

Hair, J. F., Sarstedt, M., & Ringle, C. M. (2019). Rethinking some of the rethinking of partial least squares. *European Journal of Marketing, 53*(4), 566–584. https://doi.org/10.1108/EJM-10-2018-0665.

Hale, C. (1996). Fear of crime: A review of the literature. *International Review of Victimology, 4*, 79–150.

Hamblen, M. (2015, November 12). Half of U.S. businesses have no formal BYOD policy for security. *Computer World*. https://www.computerworld.com/article/3004838/half-of-us-businesses-have-no-formal-byod-policy-for-security.html Accessed 24 March 2019.

Journal Pre-proof

Han, B. (2017). User's information security awareness in BYOD programs: A theoretical model. Paper presented at the Information Institute Conference, Las Vegas, NV. http://029e2c6.netsolhost.com/II-Proceedings/2017/IIVC2017_HAN.pdf Accessed 16 March 2019.

He, J., & Freeman, L. A. (2010). Are men more technology-oriented than women? The role of gender on the development of general computer self-efficacy of college students. *Journal of Information Systems Education, 21*, 203-212.

He, Y., Chen, Q., & Kitkuakul, S. (2018). Regulatory focus and technology acceptance: Perceived ease of use and usefulness as efficacy. *Cogent Business & Management, 5*(1), 1–22.

Helmes, A. W. (2002). Application of the protection motivation theory to genetic testing for breast cancer risk. *Preventive Medicine, 35*(5), 453–462.

Henseler, J., Ringle, C. M., & Sinkovics, R. R. (2009). The use of partial least squares path modeling in international marketing. *Advances in International Marketing, 20*(1), 277–319.

Heraldkeeper. BYOD security market 2019 size, share global emerging technologies, growth rate analysis, business strategy and trends by forecast 2023 (2019). https://www.marketwatch.com/press-release/byod-security-market-2019-size-share-global-emerging-technologies-growth-rate-analysis-business-strategy-and-trends-by-forecast-2023-2019-01-30 Accessed 16 March 2019.

Herath, T., & Rao, H. R. (2009a). Encouraging information security behaviors in organisations: Role of penalties, pressures and perceived effectiveness. *Decision Support Systems, 47*(2), 154–165.

Herath, T., & Rao, H. R. (2009b). Protection motivation and deterrence: A framework for security policy compliance in organisations. *European Journal of Information Systems, 18*(2), 106–125.

Hoehle, H., Zhang, X., & Venkatesh, V. (2015). An espoused cultural perspective to understand continued intention to use mobile applications: A four-country study of mobile social media application usability. *European Journal of Information Systems, 24*(3), 337–359.

Hofstede, G. (1980). *Culture's consequences: Comparing values, behaviours, institutions and organisations across nations*. Thousand Oaks, CA: Sage.

Hofstede, G. Compare countries. (2019). https://www.hofstede insights.com/product/compare-countries/ Accessed 24 March 2019.

Hovav, A., & Putri, F. F. (2016). This is my device! Why should I follow your rules? Employees' compliance with BYOD security policy. *Pervasive and Mobile Computing, 32*, 35–49.

Humaidi, N. & Balakrishnan, V. (2015). Leadership styles and information security compliance behavior: The mediator effect of information security awareness. *International Journal of Information and Education Technology, 5*(4), 311–318.

Ifinedo, P. (2012). Understanding information systems security policy compliance: An integration of the theory of planned behavior and the protection motivation theory. *Computers & Security, 31*(1), 83–95.

Journal Pre-proof

Ifinedo, P. (2014). Information systems security policy compliance: An empirical study of the effects of socialisation, influence, and cognition. *Information & Management*, *51*(1), 69–79.

Ifinedo, P. (2016). Critical times for organisations: what should be done to curb workers' noncompliance with IS security policy guidelines? *Information Systems Management, 33*(1), 30–41.

International Telecommunication Union. Global Cybersecurity Index (GCI) 2017. (2017). https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf Accessed 30 July 2019.

Jacobs, B. A. (2010). Deterrence and deterrability. *Criminology*, *48*(2), 417–441.

Jahangirov, N., Saglam Ari, G., Jahangirov, S., & Guneri Tosunoglu, N. (2015). The relationship between glass ceiling and power distance as a cultural variable by a new method. *International Journal of Organizational Leadership, 4*, 465–483.

Jhangiani, C., & Tarry, H. (2011). *Principles of social psychology*. https://opentextbc.ca/socialpsychology/ Accessed 24 March 2019.

Johnson, D. W., & Koch, H. (2006). Computer security risks in the internet era: Are small business owners aware and proactive? *Proceedings of the 39th Annual Hawaii International Conference on System Sciences,* Vol. 6, 130b–135b.

Johnston, A. C., & Warkentin, M. (2010). Fear appeals and information security behaviors: An empirical study. *MIS Quarterly, 34*(3), 549–566.

Kaplan, J., Sharma, S., & Weinberg, A. (2011, June). Meeting the cybersecurity challenge. *McKinsey*. https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/meeting-the-cybersecurity-challenge Accessed 13 March 2019.

Kerr, D., Talaei-Khoei, A., & Ghapanchi, A. H. (2018). A paradigm shift for bring your own device (BYOD). *Proceedings of the 24th Americas Conference on Information Systems: Digital Disruption, USA,* 1–10.

Khatri, N. (2009). Consequences of power distance orientation in organisations. *Vision, 13*(1), 1–9.

King, J., Bond, T., & Blandford, S. (2002). An investigation of computer anxiety by gender and grade. *Computers in Human Behavior, 18*(1), 69–84.

Kline, R. B., (2005). *Principles and practice of structural equation modeling*.(2nd ed), New York: Guilford Press.

Knapp, K. J., Marshall, T. E., Rainer, R. K., & Ford, F. N. (2005). Managerial dimensions in information security: A theoretical model of organisational effectiveness (ISC)2 Inc., Palm Harbor, Florida and Auburn University, Auburn, Alabama.

Kobayashi, E., & Grasmick, H. A. (2002). Comparison of the perceived threats of managerial sanctions, embarrassment and shame in Japan and the United States. *Journal of Language, Culture and Communication, 4*(1), 11–52.

Koch, S., Muller, S., & Sieverding, M. (2008). Women and computers: Effects of stereotype threat on attribution of failure. *Computers & Education, 51*(4), 1795–1803.

Journal Pre-proof

Köffer, S., Ortbach, K., & Niehaves, B. (2014). Exploring the relationship between IT consumerization and job performance: A theoretical framework for future research. *Communications of the Association for Information Systems*, *35*(1), 261–283.

Lam, T., Cho, V., & Qu, H. (2007). A study of hotel employee behavioral intentions towards adoption of information technology. *International Journal of Hospitality Management*, *26*(1), 49–65.

Latikka, R., Turja, T., & Oksanen, A. (2019). Self-efficacy and acceptance of robots. *Computers in Human Behavior*, *93*(1), 157–163.

Lazar, M. (2018, November 16). BYOD statistics provide snapshot of future. *Insight*. https://www.insight.com/en_US/learn/content/2017/01182017-byod-statistics-provide-snapshot-of-future.html Accessed 24 March 2019.

Lee, D., LaRose, R., & Rifon, N. (2008). Keeping our network safe: A model of online protection behaviour. *Journal of Behaviour & Information Technology*, *27*(5), 445–454.

Li, L., He, W., Xu, L., Ash, I., Anwar, M., & Yuan, X. (2019). Investigating the impact of cybersecurity policy awareness on employees' cybersecurity behavior. *International Journal of Information Management*, *45*, 13–24.

Lin, X., Featherman, M., Brooks, S. L., & Hajli, N. (2018). Exploring gender differences in online consumer purchase decision making: An online product presentation perspective. *Information Systems Frontiers*, 1–15. https://doi.org/10.1007/s10796-018-9831-1.

Lord, N. (2017, February 27). The ultimate guide to BYOD security: Overcoming challenges, creating effective policies, and mitigating risks to maximize benefits. *Digital Guardian*. https://digitalguardian.com/blog/ultimate-guide-byod-security-overcoming-challenges-creating-effective-policies-and-mitigating Accessed 16 March 2019.

Maddux, J. E., & Rogers, R. W. (1983). Protection motivation and self-efficacy: A revised theory of fear appeals and attitude change. *Journal of Experimental Social Psychology*, *19*(5), 469–479.

Madichie, N. O., & Gallant, M. (2012). Broken silence: A commentary on women's entrepreneurship in the United Arab Emirates. *International Journal of Entrepreneurship and Innovation*, *13*(2), 81–92.

Maitlo, A., Ameen, N., Peikari, H. R., & Shah, M. (2019). Preventing identity theft: Identifying major barriers to knowledge-sharing in online retail organisations. *Information Technology & People*. https://doi.org/10.1108/ITP-05-2018-0255

Mamonov, S., & Benbunan-Fich, R. (2018). The impact of information security threat awareness on privacy-protective behaviors. *Computers in Human Behavior*, *83*(1), 32–44.

Martens, M., De Wolf, R., & De Marez, L. (2019). Investigating and comparing the predictors of the intention towards taking security measures against malware, scams and cybercrime in general. *Computers in Human Behavior*, *92*, 139–150.

Journal Pre-proof

McCormac, A., Zwaans, T., Parsons, K., Calic, D., Butavicius, M., & Pattinson, M. (2017). Individual differences and information security awareness. *Computers in Human Behavior, 69*(1), 151–156.

McCoy, S., Everard, A. & Jones, B.M., (2005). An examination of the technology acceptance model in Uruguay and the US: A focus on culture. *Journal of Global Information Technology Management*, 8(2), 27-45.

Merhi, M. I., & Ahluwalia, P. (2019). Examining the impact of deterrence factors and norms on resistance to information systems security. *Computers in Human Behavior, 92*(1), 37–46.

Moskites, T. (2017, February 16). Who makes better cybersecurity decisions, men or women? *CSO Online*. https://www.csoonline.com/article/3153149/who-makes-better-cybersecurity-decisions-men-or-women.html Accessed 24 March 2019.

Musarurwa, A., Flowerday, S., & Cilliers, L. (2017). Individual traits that determine the bring your own device information security culture: A case study of the banking sector in Zimbabwe. In G. Dhillon, & S. Samonas (Eds.), *Proceedings of the 16th Annual Security Conference: Discourses in Cyber Security*, USA, 1–18.

Neuwirth, K., Dunwoody, S., & Griffin, R. J. (2000). Protection motivation and risk communication. *Risk Analysis, 20*(5), 721–734.

Öğütçü, G., Testik, Ö. M., & Chouseinoglou, O. (2016). Analysis of personal information security behavior and awareness. *Computers & Security*, *56*(1), 83–93.

Ong, C. S., & Lai, J. Y. (2006). Gender differences in perceptions and relationships among dominants of e-learning acceptance. *Computers in Human Behavior, 22*(5), 816–829.

Onumo, A., Cullen, A., & Ullah-Awan, I. (2017). An empirical study of cultural dimensions and cybersecurity development. *Proceedings of the 5th International Conference on Future Internet of Things and Cloud (FiCloud),* Prague, 70–76. doi: 10.1109/FiCloud.2017.41.

Paternoster, R., Saltzman, L. E., Waldo, G. P., & Chiricos, T. G. (1985). Assessments of risk and behavioral experience: An exploratory study of change. *Criminology*, *23*(3), 417–436.

Pewinternet. Mobile fact sheet. (2018). http://www.pewinternet.org/fact-sheet/mobile/ Accessed 24 March 2019.

Pitichat, T. (2013). Smartphones in the workplace: Changing organisational behavior, transforming the future. *LUX: A Journal of Transdisciplinary Writing and Research from Claremont Graduate University*, *3*(1), 1–13.

Putri, F., & Hovav, A. (2014). Employees' compliance with BYOD security policy: Insights from reactance, organizational justice, and protection motivation theory. *Proceedings of the European Conference on Information Systems (ECIS), Israel.* ISBN 978-0-9915567-0-0

PWC. Global top 100 companies by market capitalization. (2017). https://www.pwc.com/gx/en/audit-services/assets/pdf/global-top-100-companies-2017-final.pdf Accessed 24 March 2019.

Journal Pre-proof

Rogers, R. W. (1975). A protection motivation theory of fear appeals and attitude change. *The Journal of Psychology, 91*(1), 93–114.

Rogers, R. W. (1983). Cognitive and physiological processes in fear appeals and attitude change: A revised theory of protection motivation. In J. Cacioppo, & R. Petty (Eds.), *Social psychophysiology* (pp. 153–176). New York, NJ: Guilford Press.

Romer, H. (2014). Best practices for BYOD security. *Computer Fraud & Security*, 14 (1), 13–15.

Siponen, M., Pahnila, S., & Mahmood, A. (2006). Factors influencing protection motivation and IS security policy compliance. *Proceedings of the 2006 Innovations in Information Technology, Dubai,* 1–5. IEEE. doi: 10.1109/INNOVATIONS.2006.301907.

Siponen, M., Pahnila, S., & Mahmood, M. (2010). Compliance with information security policies: An empirical investigation. *Computer, 43*(2), 64–71.

Srite, M., & Karahanna, E. (2006). The role of espoused national cultural values in technology acceptance. *MIS Quarterly, 30*(3), 679–704.

Sriwindono, H., & Yahya, S. (2014). The influence of cultural dimension on ICT acceptance in Indonesia higher learning institution. *Australian Journal of Basic and Applied Sciences, 8*(5), 215–225.

Stedham, Y., & Yamamura, J. (2002). National cultural characteristics: A comparison of gender differences in Japan and the US. *Proceedings of the Academy of Business and Administrative Studies International Conference,* Costa Rica. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.514.5184&rep=rep1&type=pdf.

Tarhini, A., Elyas, T., Akour, M. A., & Al-Salti, Z. (2016). Technology, demographic characteristics and e-learning acceptance: A conceptual model based on extended technology acceptance model. *Higher Education Studies, 6*(3), 72–89.

Tarhini, A., Hone, K., & Liu, X. (2014). Measuring the moderating effect of gender and age on e-learning acceptance in England: A structural equation modeling approach for an extended technology acceptance model. *Journal of Educational Computing Research, 51*(2), 163–184.

Tarhini, A., Hone, K., & Liu, X. (2015). A cross-cultural examination of the impact of social, organisational and individual factors on educational technology acceptance between British and Lebanese university students. *British Journal of Educational Technology, 46*(4), 739–755.

Timms, K. (2017). BYOD must be met with a wider appreciation of the cyber-security threat. *Computer Fraud & Security, 3*(7), 5–8.

Trade Arabia. (2016, April 12). BYOD, mobility trends "continue to impact UAE businesses". *Trade Arabia*. http://www.tradearabia.com/news/IT_304803.html Accessed 16 March 2019.

Triandis, H. C. (1989). The self and social behaviour in differing cultural contexts. *Psychological Review, 96*(1), 506–520.

Journal Pre-proof

Tu, C. Z., Adkins, J., & Zhao, G. Y. (2018). Complying with BYOD security policies: A moderation model. *Proceedings of the Midwest Association for Information System (MWAIS) 25*. Doi: 10.17705/3jmwa.000045.

Übelacker, S. (2013). Security-aware organisational cultures as a starting point for mitigating socio-technical risks. In M. Horbach (Ed.), *Informatik 2013* (pp. 2046–2057). Lecture Notes in Informatics (LNI): Vol. P-220. https://doi.org/10.15480/882.1130.

Ubene, O. I. E., Agim, U. R., & Umo-Odiong, A. (2018). The impact of bring your own device (BYOD) on information technology (IT) security and infrastructure in the Nigerian insurance sector. *American Journal of Engineering Research, 7*(5), 237–246.

United States Department of Labor. Data and statistics: Women in the labor force. (2019). https://www.dol.gov/wb/stats/stats_data.htm Accessed 16 March 2019.

Vaidya, R. Cyber security breaches survey. (2018). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/702074/Cyber_Security_Breaches_Survey_2018_-_Main_Report.pdf Accessed 28 March 2019.

van Bavel, R., Rodríguez-Priego, N., Vila, J., & Briggs, P. (2019). Using protection motivation theory in the design of nudges to improve online security behavior. *International Journal of Human-Computer Studies, 12*(3), 29–39.

Van Der Pligt, J., (1998). Perceived risk and vulnerability as predictors of precautionary behaviour. *British journal of health psychology*, 3(1), 1-14.

Van Schaik, P., Jeske, D., Onibokun, J., Coventry, L., Jansen, J., & Kusev, P. (2017). Risk perceptions of cyber-security and precautionary behaviour. *Computers in Human Behavior, 75*(1), 547–559.

Vance, A., Siponen, M., & Pahnila, S. (2012). Motivating IS security compliance: Insights from habit and protection motivation theory. *Information & Management, 49*(4), 190–198.

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of information technology: Toward a unified view. *MIS Quarterly, 27*(3), 425–478.

Venkatesh, V., Thong, J. Y., & Xu, X. (2012). Consumer acceptance and use of information technology: Extending the unified theory of acceptance and use of technology. *MIS Quarterly, 36*(1), 157–178.

Vujovic, K.S., Vuckovic, S., Vujovic, A. & Prostran, M., (2016). The analgesic efficacy of ketamine-magnesium combination is influenced by the order of medication administration. *European Psychiatry, 33*(1), S290–S643.

Weber, L., & Rudman, R. J. (2018). Addressing the incremental risks associated with adopting bring your own device. *Journal of Economic and Financial Sciences, 11*(1), a169. https://doi.org/10.4102/jef.v11i1.169.

Willison, R., Warkentin, M., & Johnston, A. C. (2018). Examining employee computer abuse intentions: Insights from justice, deterrence and neutralization perspectives. *Information Systems Journal, 28*(2), 266–293.

Wong, K. T., Teo, T., & Russo, S., (2012). Influence of gender and computer teaching efficacy on computer acceptance among Malaysian student teachers: An extended

Journal Pre-proof

technology acceptance model. *Australasian Journal of Educational Technology, 28*(7), 1190–1207.

Woon, I., Tan, G. W., & Low, R. (2005). A protection motivation theory approach to home wireless security. In International Conference on Information Systems pp 367–380 Las Vegas, USA.

World Bank. Labor force participation rate, female (% of female population ages 15+) (modeled ILO estimate) (2018). https://data.worldbank.org/indicator/SL.TLF.CACT.FE.ZS Accessed 24 March 2019.

Zahadat, N., Blessner, P., Blackburn, T., & Olson, B. A. (2015). BYOD security engineering: A framework and its analysis. *Computers & Security, 55*, 81–99.

Zeffane, R. (2017). Gender, individualism–collectivism and individuals' propensity to trust: A comparative exploratory study. *Journal of Management & Organization*. Advance online publication. https://doi.org/10.1017/jmo.2017.57.

Zeldin, A. L., Britner, S. L., & Pajares, F. (2008). A comparative study of the self□efficacy beliefs of successful men and women in mathematics, science, and technology careers. *Journal of Research in Science Teaching, 45*(9), 1036–1058.

Journal Pre-proof

Journal Pre-proof

Highlights

- BYOD is becoming popular among the Gen-Mobile workforce and it introduces cybersecurity threats
- There is a growing business concern about the threats posed by these devices
- Male and female employees in US and UAE do not find their organisations' recommendations effective
- A new model combining PMT, GDT and Hofstede's cultural dimensions was developed

Journal Pre-proof